REMARKS

Applicants have carefully reviewed the Application in light of the Office Action dated April 4, 2008 (the "Office Action"). Claims 20-48, 55-59, 63-73, 85-99, 104-107, and 113-118 were previously withdrawn from consideration. Claim 19 has been cancelled. Claims 1, 49, 51, 53-54, 60-61, 74, 100, 108, and 111-112 are amended as set forth above. Thus, claims 1-18, 49-54, 60-62, 74-84, 100-103 and 108-112 remain pending in the application. Applicants submit that no new matter has been added with the amendments. Applicants respectfully request reconsideration of the application in accordance with the following remarks.

Election/Restrictions

Applicants affirm that responsive to the action mailed September 10, 2007 ("Restriction Requirement"), Group I (claims 1-19, 49-54, 60-62, 74-84, 100-103, and 108-112) was elected without traverse in Applicants' response mailed January 10, 2008. Therefore, Groups II-VI as identified by the Restriction Requirement (comprising claims 20-48, 55-59, 63-73, 85-99, 104-107, and 113-118) have been withdrawn from consideration.

Section 103 Rejections

Claims 1-19, 49-54, 60-62, 74-84, 100-103, and 108-112 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,502,766 to Boebert et al. ("*Boebert*") in view of U.S. Patent No. 6,226,618 to Downs et al. ("*Downs*"). Applicants respectfully traverse the rejections and all the assertions and holdings therein, and submit that it has not been shown that the cited references of *Boebert* and *Downs*, either alone or in combination, teach, suggest, or disclose each and every element of the present claims. Thus, Applicants respectfully submit that the claims are patentable over the cited art.

Independent Claims 1 and 74:

Claim 1 recites:

> A method for managing digital rights, the method comprising:

detecting a data file on a user device, wherein the data file includes a digital wrapper preventing access to the data file without a valid authorization;

determining whether the user device includes software for disabling the digital wrapper, with the determination being made using executable instructions associated with the digital wrapper;

searching for information relating to an authorization to access the data file using data stored in a non-volatile storage area of the user device;

identifying information relating to an authorization to access the data file; and

disabling the digital wrapper based on the authorization.

Applicants submit that it has at least not been shown that either *Boebert* or *Downs* teaches, suggests, or discloses each and every element of claim 1. For example, claim 1, as amended, recites "determining whether the user device includes software for disabling the digital wrapper, with the determination being made using executable instructions associated with the digital wrapper." A similar, but different, claim element was previously included in originally filed (and now cancelled) claim 19. The Office Action referenced FIGURE 33 of *Boebert* to reject the claim. Office Action, p. 10.[1] *Boebert* describes FIGURE 33, and the Authentication Token Exchange Protocol it embodies, as being used to determine whether incoming transactions were properly "chained" to an outgoing message. *Boebert*, 28:14-24. In other words, the token exchange is used to ensure that incoming transactions are not erroneous or forged, and "to differentiate masquerade attempts from alarms caused by faulty transmission or equipment failures." *Id.* at 27:20-28; 28:14-24. If a certain number of transmissions fails to provide a match between the token received and the token that should have been received, then an alarm may be raised. *Id.* Thus, FIGURE 33 describes a method of authenticating messages sent between devices in the *Boebert* system, and clearly fails to teach or suggest the claim 1 element of determining whether the user device includes software for disabling the digital wrapper using executable instructions associated with the digital wrapper. Therefore, it has not been shown that the *Boebert-Downs* combination teaches or suggests each and every element of claim 1.

Accordingly, Applicants respectfully request reconsideration and allowance of amended claim 1 and all claims depending therefrom. Further, claim 74, as amended, includes certain

[1] "FIGURE 33 is a flow diagram detailing the steps used by the Authentication Token Exchange Protocol to 'chain' together transactions of other protocols in Trusted Path operation." *Boebert*, 8:40-44.

aspects analogous to claim 1 and is allowable for at least the reasons discussed above. Therefore, Applicants respectfully request reconsideration and allowance of claim 74 and all claims depending therefrom.

Independent Claims 49 and 100:

Claim 49 recites:

> A method for managing digital rights, the method comprising:
>
> monitoring an input/output system of a user device for attempted file transfers between the user device and an external device through one or more input/output ports of the user device;
>
> detecting an attempt to transfer a data file between the user device and an external device through one of the input/output ports of the user device, wherein the data file is stored in an unwrapped form prior to the attempt to transfer the data file; and
>
> applying a digital wrapper to the unwrapped data file in response to the detected attempt to transfer the data file before allowing the attempted transfer, wherein the digital wrapper is adapted to prevent unauthorized access to the data file after the data file is transferred between the user device and the external device.

Applicants submit that it has at least not been shown that either *Boebert* or *Downs* teaches, suggests, or discloses each and every element of claim 49. For example, claim 49 recites "detecting an attempt to transfer a data file between the user device and an external device" where the data file is stored in an unwrapped form prior to the attempt to transfer the data file, and, in response to the detected transfer attempt, applying a digital wrapper to the data file.

Generally, Claim 49 is directed to the problem of preventing data files from being copied off of a user device to some external device where the data file is subject to unauthorized access, while still allowing the data file to remain freely accessible within a user device on which it resides for authorized use. Accordingly, when a transfer of a data file is attempted, the file is wrapped to prevent unauthorized access after the file is actually transferred. Thus, after the transfer, access to the file can be limited to authorized users and/or authorized devices by the applied digital wrapper.

It has at least not been shown that either *Boebert* or *Downs* disclose or suggest storing a data file in an unwrapped form on a user device prior to an attempt to transfer the data file and applying a digital wrapper to the unwrapped data file in response to detecting an attempt to transfer the data file before allowing the attempted transfer. *Boebert*, for instance, is directed to a data communication system including a secure processing unit that communicates with a personal keying device and a crypto media controller attached to a user's computer. *Boebert*, Abstract. Communication between elements of the system creates keys, identifiers, and attributes used to identify and authenticate the user, assign user security access rights and privileges, and assign media and device attributes to a data access device according to a predefined security policy. *Id.* Further, *Boebert* seems to at least teach away from storing a data file in an unwrapped form on a user device prior to an attempt to transfer the data file, instead teaching that access to files within a unit of media is allowed only "at the last possible moment" using a "combination of an 'access vector' assigned to an individual and the 'device attributes' assigned to a particular Workstation." *Id.* at 3:20-24. In other words, *Boebert's* media is stored in encrypted form before, during, and after any transfer. Thus, *Boebert* has not been shown to teach or suggest that files are stored in an unwrapped form on a user device, where a digital wrapper is applied to the file in response to detecting an attempt to transfer the data file.

Downs, on the other hand, discloses a system and related tools for the secure delivery and rights management of digital assets. *Downs*, Abstract. However, *Downs* explicitly teaches away from the claim 49 elements of storing a data file in unwrapped form and in response to an attempt to transfer the data file, applying the digital wrapper. Instead, *Downs* teaches that the enforcement of content usage conditions is performed by the following steps:

> "First, upon reception of the Content 113 copy…the End-User Device(s) 109 marks the Content 113 with a Copy/Play Code 523 representing the initial copy/play permission. Second, the Player Application 195 cryptographically scrambles the Content 113 before storing it in the End-User Device(s) 109. The Player Application 195 generates a scrambling key for each Content Item, and the key is encrypted and hidden in the End-User Device(s) 109. Then, every time the End-User Device(s) 109 accesses the Content 113 for copy or play, the End-User Device(s) 109 verifies the copy/play code before allowing the de-scrambling of the Content 113 and the execution of the play or copy."

Downs, 21:43-63 (emphasis added). In direct contrast to claim 49, *Downs* teaches that content is encrypted and stored (in an encrypted form) on the user device immediately upon receiving the content, requiring the content to be decrypted and verified before any access for copy or play. Thus, the content is not "stored in an unwrapped form prior to the attempt to transfer the [content]" and wrapped "in response to a detected attempt to transfer the [content]" as recited by claim 49. Therefore, it has not been shown that the *Boebert-Downs* combination teaches or suggests each and every element of claim 49.

Accordingly Applicants respectfully request reconsideration and allowance of amended claim 49 and all claims depending therefrom. Further, claim 100, as amended, includes certain aspects analogous to claim 49 and is allowable for at least the reasons discussed above. Therefore, Applicants respectfully request reconsideration and allowance of claim 100 and all claims depending therefrom.

Independent Claims 60 and 108:

Claim 60 recites:

> A method for managing digital rights, the method comprising:
> identifying a media file stored on a user device for distribution to an external device, where the media file is stored in an unwrapped form prior to distribution;
> identifying access rules associated with the media file, wherein the access rules include information relating to usage rights and usage fees;
> applying a digital wrapper to the media file before distribution occurs, with the digital wrapper including identification data for the media file and data relating to the access rules, wherein the digital wrapper is adapted to prevent unauthorized access to the media file after the media file is distributed to the external device.

Claim 60 recites identifying a media file stored on a user device for distribution to an external device, where the media file is stored in an unwrapped form prior to distribution, and where a digital wrapper is then applied to the file before the distribution occurs. As discussed with regards to claim 49, the *Boebert-Downs* combination has not been shown to teach or suggest a media file that "is stored in an unwrapped form [on the user device] prior to distribution," and where a "digital wrapper [is applied] to the media file before the distribution

occurs." For at least these reasons, Applicants respectfully request reconsideration and allowance of amended claim 60 and all claims depending therefrom. Further, claim 108, as amended, includes certain aspects analogous to claim 60 and is allowable for at least the reasons discussed above. Therefore, Applicants respectfully request reconsideration and allowance of claim 108 and all claims depending therefrom.

CONCLUSION

It is believed that all of the pending claims have been addressed. However, the absence of a reply to a specific rejection, issue or comment does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

No fees are believed to be due at this time. If any extension of time is required, Applicants hereby request the appropriate extension of time. Please apply any other charges or credits to Deposit Account No. 06-1050.

Respectfully submitted,

Date: July 7, 2008

/Spencer C. Patterson/
Spencer C. Patterson
Reg. No. 43,849

PTO Customer No. 26231
Fish & Richardson P.C.
1717 Main Street, Suite 5000
Dallas, Texas 75201
Telephone: (214) 292-4082
Facsimile: (214) 747-2091